(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 199 36 939 A 1**

(51) Int. Cl.[7]:
G 06 F 12/14
G 06 K 19/073
G 09 C 1/00

(21) Aktenzeichen: 199 36 939.9
(22) Anmeldetag: 5. 8. 1999
(43) Offenlegungstag: 6. 4. 2000

DE 199 36 939 A 1

(66) Innere Priorität:
198 44 992. 5 30. 09. 1998

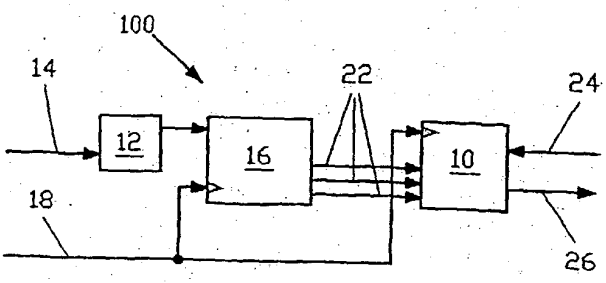
(71) Anmelder:
Philips Corporate Intellectual Property GmbH, 22335 Hamburg, DE

(72) Erfinder:
Feuser, Markus, Dr., 21244 Buchholz, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Datenverarbeitungseinrichtung und Verfahren zu dessen Betrieb zum Verhindern einer differentiellen Stromverbrauchanalyse

(57) Die vorliegende Erfindung betrifft eine Datenverarbeitungseinrichtung (100) sowie ein Verfahren zum Betreiben einer Datenverarbeitungseinrichtung, insbesondere einer Chipkarte, mit einer integrierten Schaltung, welche in Abhängigkeit von einem Taktsignal Rechenoperationen, insbesondere kryptographische Operationen, Datenein- bzw. -ausgaben sowie eine Datenübergabe von bzw. zu Registern der integrierten Schaltung ausführt. Hierbei wird die integrierte Schaltung (10) derart gesteuert, dass das Ausführen von Rechenoperationen einerseits und die Datenein-/-ausgabe sowie die Datenübergabe von Register zu Register bzw. zwischen Registern andererseits zeitlich parallel durchgeführt wird.



DE 199 36 939 A 1

Beschreibung

Technisches Gebiet

Die Erfindung betrifft ein Verfahren zum Betreiben einer Datenverarbeitungseinrichtung, insbesondere einer Chipkarte, mit einer integrierten Schaltung, welche in Abhängigkeit von einem Taktsignal Rechenoperationen, insbesondere kryptographische Operationen, Datenein- bzw. -ausgaben sowie eine Datenübergabe zwischen Registern der integrierten Schaltung ausführt, gemäß dem Oberbegriff des Anspruchs 1. Die Erfindung betrifft ferner eine Datenverarbeitungseinrichtung, insbesondere Chipkarte, insbesondere zum Ausführen des Verfahrens, mit einer integrierten Schaltung, welche in Abhängigkeit von einem Taktsignal Rechenoperationen, insbesondere kryptographische Operationen, ausführt, wobei die integrierte Schaltung ein Rechenwerk mit zugeordnetem ersten Register und Datenein- und -ausgängen aufweist, gemäß dem Oberbegriff des Anspruchs 3.

Stand der Technik

In vielen Datenverarbeitungsgeräten mit integrierter Schaltung dienen beispielsweise kryptographische Operationen zum Schutz des Betriebes dieser Geräte bzw. zum Schutz von in dem Gerät transportierten Daten. Die hierfür notwendigen Rechenoperationen werden dabei sowohl von Standard-Rechenwerken als auch von dedizierten Crypto-Rechenwerken durchgeführt. Ein typisches Beispiel für letzteres sind Chipkarten bzw. IC-Karten. Bei in diesem Zusammenhang verwendeten Daten bzw. Zwischenergebnissen handelt es sich üblicherweise um sicherheitsrelevante Informationen, wie beispielsweise kryptographische Schlüssel oder Operanden.

Bei von der integrierten Schaltung durchgeführten Rechenoperationen, beispielsweise zur Berechnung von kryptographischen Algorithmen, werden logische Verknüpfungen zwischen Operanden bzw. Zwischenergebnissen durchgeführt. In Abhängigkeit von der verwendeten Technologie führen diese Operationen, insbesondere das Laden von leeren oder zuvor gelöschten Speicherbereichen bzw. Register mit Daten, zu einem erhöhten Stromverbrauch der Datenverarbeitungsgeräte. Bei komplementärer Logik, wie beispielsweise der CMOS-Technik, tritt ein erhöhter Stromverbrauch dann auf, wenn der Wert einer Bit-Speicherzelle geändert wird, d. h. sein Wert sich von "0" auf "1" bzw. von "1" auf "0" ändert. Der erhöhte Verbrauch hängt dabei von der Anzahl der im Speicher bzw. Register geänderten Bitstellen ab. Mit anderen Worten lässt das Laden eines zuvor gelöschten Registers einen Stromverbrauch proportional zum Hamminggewicht des in das leere Register geschriebenen Operanden (= Anzahl der Bits mit dem Wert "1") ansteigen. Durch eine entsprechende Analyse dieser Stromänderung könnte es möglich sein, Informationen über die berechneten Operationen zu extrahieren, so dass eine erfolgreiche Kryptoanalyse von geheimen Operanden, wie beispielsweise kryptographischen Schlüsseln, möglich ist. Mittels Durchführung mehrerer Strommessungen am Datenverarbeitungsgerät könnten beispielsweise bei sehr kleinen Signaländerungen eine hinreichende Extraktion der Informationen ermöglicht werden. Andererseits könnten mehrere Strommessungen eine ggf. erforderliche Differenzbildung ermöglichen. Diese Art der Kryptoanalyse wird auch als "Differential Power Analysis" bezeichnet, mittels derer ein Außenstehender durch reine Beobachtung von Änderungen des Stromverbrauches des Datenverarbeitungsgerätes eine ggf. unberechtigte Kryptoanalyse der kryptographischen Operationen, Algorithmen, Operanden bzw. Daten erfolgreich ausführen kann. Die "Differential Power Analysis" ermöglicht somit über eine reine Funktionalität hinaus zusätzliche interne Informationen einer integrierten Schaltung gewinnen zu können.

Aus der US 5 297 201 ist es bekannt, einen Hochfrequenz abstrahlenden Computer mit einer Einrichtung zu kombinieren, welche ebenfalls eine Hochfrequenz ähnlich zu derjenigen des Computers abstrahlt. Dadurch ist es für einen unberechtigten Dritten nicht mehr möglich, die Hochfrequenzabstrahlung des Computers zu dekodieren. Eine Kryptoanalyse durch einen Dritten, der unmittelbar Zugang zum Computer hat, kann dieses System jedoch nicht verhindern.

Die WO 90/15489 beschreibt ein gesichertes Kommunikationssystem, bei dem Dummyverkehr bzw. -übertragungen erzeugt werden, um kryptographische Analysen zu erschweren. Eine Kryptoanalyse durch einen Dritten, der unmittelbar Zugang zum Computer hat, kann dieses System jedoch ebenfalls nicht verhindert werden.

Darstellung der Erfindung, Aufgabe, Lösung, Vorteile

Es ist Aufgabe der vorliegenden Erfindung, ein verbessertes Verfahren und eine verbesserte Datenverarbeitungseinrichtung der obengenannten Art zur Verfügung zu stellen, welche die obengenannten Nachteile beseitigen und einen wirksamen Schutz gegen eine "Differential Power Analysis" zur Verfügung stellen.

Diese Aufgabe wird durch ein Verfahren der o. g. Art mit den in Anspruch 1 gekennzeichneten Merkmalen und durch eine Datenverarbeitungseinrichtung der o. g. Art mit den in Anspruch 3 gekennzeichneten Merkmalen gelöst.

Dazu ist es bei dem Verfahren der o. g. Art erfindungsgemäß vorgesehen, dass die integrierte Schaltung derart gesteuert wird, dass das Ausführen von Rechenoperationen einerseits und die Datenein-/-ausgabe sowie die Datenübergabe von Register zu Register bzw. zwischen Registern andererseits zeitlich parallel durchgeführt wird.

Dies hat den Vorteil, dass für eine "Differential Power Analysis" Anhaltspunkte dafür fehlen, wann eine Rechenoperation endet bzw. wann ein Auslesen/Beschreiben von Registern oder wann eine Datenein-/-ausgabe erfolgt, da Zeitbereiche sowohl der eigentlichen Berechnungen als auch der Datenein- und Datenausgabe verschleiert werden. Die "Differential Power Analysis" wird somit erheblich erschwert, da von außen nicht mehr festgestellt werden kann, ob eine wirkliche Berechnung oder eine Ein-/Ausgabe stattfindet.

In einer vorteilhaften Weiterbildung des Verfahrens werden zum weiteren Verschleiern der Rechenoperationen sowie Datenein-/Ausgaben unmittelbar vor, während und/oder unmittelbar nach der Datenübergabe zwischen den Registern der integrierten Schaltung Dummyberechnungen von einem Rechenwerk der integrierten Schaltung ausgeführt, welche zufällige oder vorbestimmte Daten bearbeiten, wobei keine Daten in Register der integrierten Schaltung geschrieben werden.

Bei einer Datenverarbeitungseinrichtung der o. g. Art ist es erfindungsgemäß vorgesehen, dass ein mit dem ersten Register verbundenes zweites Register vorgesehen ist, welches die Datenein- und -ausgänge aufweist, wobei ferner eine Steuereinheit mit der integrierten Schaltung verbunden ist, welche derart ausgebildet ist, dass sie einen zeitlich parallelen Betrieb der Register zur Datenein-/-ausgabe und Datenübergabe zwischen den Registern einerseits und Rechenoperationen der Recheneinheit andererseits steuert.

Dies hat den Vorteil, dass für eine "Differential Power Analysis" Anhaltspunkte dafür fehlen, wann eine Rechenoperation endet bzw. wann ein Auslesen/Beschreiben von

Registern oder wann eine Datenein-/-ausgabe erfolgt, da Zeitbereiche sowohl der eigentlichen Berechnungen als auch der Datenein- und Datenausgabe verschleiert werden. Durch das zweite Register ist eine Ein-/Ausgabe von Daten möglich, während das Rechenwerk aktiv ist und ggf. Daten in das erste Register schreibt oder Daten aus dem ersten Register ausliest. Die "Differential Power Analysis" wird somit erheblich erschwert, da von außen bei geeigneter Ansteuerung des zweiten Registers nicht mehr festgestellt werden kann, ob eine wirkliche Berechnung oder eine Ein-/Ausgabe stattfindet.

In einer vorteilhaften Weitergestaltungen der Datenverarbeitungseinrichtung ist das erste Register ein Operandenregister des Rechenwerkes und/oder das zweite Register ein Operandenregister der Datenein-/-ausgabe.

Kurze Beschreibung der Zeichnungen

Nachstehend wird die Erfindung anhand der beigefügten Zeichnungen näher erläutert. Diese zeigen in

Fig. 1 ein Blockschaltbild einer bevorzugten Ausführungsform einer erfindungsgemäßen Datenverarbeitungseinrichtung,

Fig. 2 ein Blockschaltbild einer integrierten Schaltung der Datenverarbeitungseinrichtung von **Fig.** 1,

Fig. 3 eine graphische Veranschaulichung der Aktivität der erfindungsgemäßen Datenverarbeitungseinrichtung über die Zeit gemäß dem Stand der Technik und

Fig. 4 eine graphische Veranschaulichung der Aktivität der erfindungsgemäßen Datenverarbeitungseinrichtung über die Zeit gemäß der Erfindung.

Bester Weg zur Ausführung der Erfindung

Fig. 1 zeigt eine bevorzugte Ausführungsform einer erfindungsgemäßen Datenverarbeitungseinrichtung **100** mit einer integrierten Schaltung **10**, einem Register **12** mit Programmzugriff **14** und einer Steuereinheit **16**. Über Leitung **18** erhält die Steuereinheit **16** sowie die integrierte Schaltung ein in **Fig.** 3 und 4 dargestelltes Taktsignal **20**. Über Steuerleitungen **22** steuert die Steuereinheit **16** die integrierte Schaltung **10**, die Dateneingänge **24** und Datenausgänge **26** aufweist.

Wie aus **Fig.** 2 ersichtlich ist umfasst die integrierte Schaltung **10** ein Rechenwerk **28**, ein dem Rechenwerk **28** zugeordnetes erstes Operandenregister **30** und ein mit dem ersten Operandenregister **30** verbundenes zweites Operandenregister **32**. Die Dateneingänge **24** und Datenausgänge **26** sind am zweiten Operandenregister **32** angeordnet. Das Taktsignal **20** (**Fig.** 3 und 4) wird über die Leitung **18** sowohl an das Rechenwerk **28** als auch an die beiden Operandenregister **30** und **32** weitergeleitet. Bei Ausführung von Berechnungen bzw. Operationen durch das Rechenwerk **28** liest dieses aus dem ersten Register **30** Daten aus bzw. schreibt ein Ergebnis einer Berechnung in das erste Register **30** ein. Zwischen den Registern **30** und **32** erfolgt ein entsprechender Datenaustausch bzw. eine gegenseitige Datenübergabe, nachfolgend als R2-1 bezeichnet, wenn Daten von dem zweiten Register **32** an das erste Register **30** übergeben werden, bzw. als R1-2 bezeichnet, wenn Daten von dem ersten Register **30** an das zweite Register **32** übergeben werden. Eine der von der Steuereinheit **16** kommenden Steuerleitung **22** ist mit dem zweiten Register **32** zu dessen Steuerung verbunden, während eine andere Steuerleitung **22** mit dem ersten Register **30** zu dessen Steuerung verbunden ist.

Eine von Paul Köcher im Internet unter http://www.cryptography.com/dpa veröffentlichte "Differential Power Analysis" hat den Ansatz, dass neben den Ein/Ausgangssignalen zusätzlich eine Stromaufnahme I_a bzw. Spannungseinbrüche ΔU_a einer Versorgungsspannung U_a der integrierten Schaltung analysiert werden. Der Erfolg dieser Analysemethode hängt davon ab, ob man eine Anzahl N_A von analogen ($I_a(t)$ oder $\Delta U_a(t)$) Signalverläufen $S(k,t)$ über die Zeit mit $k = \{1, \ldots, N_A\}$ unterschiedlichen Operanden derart aufnehmen kann, dass eine Summenbildung der Form

$$T(i,t) = \sum_{k=1}^{N_A} p(i,k) \cdot S(k,t)$$

mit den Koeffizienten $p(i,k)$ mit $i = \{0, 1, 2, \ldots\}$ möglich ist. Betrachtet man unterschiedliche Signalverläufe $S(k_1,t_1)$, $S(k_2,t_1)$, $S(k_3,t_1)$... zum gleichen Zeitpunkt $t = t_1$, kann eine "Differential Power Analysis" nur funktionieren, wenn die integrierte Schaltung in diesem Moment die gleiche Rechenoperation mit unterschiedlichen Operanden $k = \{1, \ldots, N_A\}$ ausführt, d. h. die Signalverläufe $S(k,t)$ müssen genau übereinandergelegt werden können. Dieses gilt nicht nur für die Berechnung selbst, sondern auch für die Ein- und Ausgabe von Daten.

Die Erfindung verschleiert sowohl die Zeitbereiche, der eigentlichen Berechnung als auch die Zeitbereiche der Datenein- bzw. Datenausgabe. Bei geeigneter Ansteuerung des zweiten Registers **32** kann von außen nicht mehr festgestellt werden, wann eine wirkliche Berechnung oder eine Ein-/Ausgabe stattfindet. Die "Differential Power Analysis" wird somit erheblich erschwert. Die integrierte Schaltung **10** ist erfindungsgemäß mit den beiden Operandenregistern **30** und **32** ausgestattet. Diese erlauben eine Ein- und Ausgabe von Daten über das zweite Operandenregister **32** mit dessen Dateneingängen **24** und Datenausgängen **26** auch während das Rechenwerk **28** unter Nutzung des ersten Operandenregisters **30** aktiv ist und Berechnungen bzw. Operationen ausführt.

Fig. 4 veranschaulicht eine Betriebsweise der erfindungsgemäßen Datenverarbeitungseinrichtung **100**, wobei über eine Zeitachse **34** das Taktsignal **20** und ein Betriebszustand von Rechenwerk bzw. Operandenregistern angegeben ist. Hierbei bezeichnet **36** einen Betriebszustand, bei dem das Rechenwerk eine Berechnung ausführt. Mit **38** ist ein Betriebszustand bezeichnet, bei dem eine Datenein- bzw. Datenausgabe stattfindet, mit **40** ist ein Betriebszustand bezeichnet, bei dem eine Datenübergabe R1-2 stattfindet und mit **42** ist ein Betriebszustand bezeichnet, bei dem eine Datenübergabe R2-1 stattfindet.

Fig. 3 veranschaulicht in einer zu **Fig.** 3 analogen Darstellung zum Vergleich eine Betriebsweise einer herkömmlichen Datenverarbeitungseinrichtung. Hier sind die Ein- bzw. Ausgabephasen **38** der eigentlichen Berechnung **36** zeitlich vor- bzw. nachgeschaltet. Bei der "Differential Power Analysis" können die Phasen der Berechnungen **36** und der Ein-/Ausgabe **38** leicht identifiziert werden, insbesondere welche Eingaben **38** bei einer Berechnung **40** Verwendung finden und welche Ausgaben **38** die Folge sind.

Bei der in **Fig.** 4 dargestellten, erfindungsgemäßen Betriebsweise werden mittels der Steuereinheit **16** die Berechnungen **36** sowie die Datenein-/-ausgaben **38**, **40**, **42** dadurch verschleiert, dass der Datenfluss der beiden Operandenregister **30**, **32** zeitlich parallel zu den Berechnungen **36** gesteuert wird. Berechnungen **36** finden immer statt. Ob aber eine Berechnung **40** von der Eingabe **38** abhängt oder eine Ausgabe **38** liefert, wird durch die Kopieraktionen R1-2 **40** und R2-1 **42** bestimmt. Die Berechnungen vor R2-1 **42** bzw. nach R1-2 **40** sind beispielsweise Dummyberechnungen. Dummyrechenoperationen sind solche Rechenopera-

tionen, welche vorbestimmte oder zufällig gewählte Eingangsdaten bearbeiten, wobei das Ergebnis verworfen wird und nicht in die Ergebnisse bzw. Eingangsdaten der wirklichen Rechenoperationen eingehen. Zusätzliche Dummyein-/-ausgaben sind ferner optional vorgesehen. Sowohl die Dummyberechnungen als auch die Dummyeingaben/Dummyausgaben erzeugen Strom- bzw. Spannungsänderungen, welche denen der wirklichen Berechnungen und Ein-/Ausgaben sehr ähnlich sind.

Die erfindungsgemäß zum Schutz der integrierten Schaltungsteile **10** gegen "Differential Power Analysis" vorgesehene Steuereinheit **16** zielt speziell auf die Ein-/Ausgabephasen **38, 40, 42** einer in den integrierten Schaltungsteilen **10** mit Hilfe digitaler, elektronischer Signalverarbeitung durchzuführenden Berechnungen **36** ab, da auch Ein-/Ausgaben anhand des Stromverbrauches mittels der "Differential Power Analysis" analysiert werden könnten. Entsprechend ist bei der "Differential Power Analysis" von Interesse, wann eine Berechnung **36** beginnt oder endet. Genau diese Informationen werden von dem erfindungsgemäßen Verfahren bzw. bei der erfindungsgemäßen Vorrichtung im Stromverbrauchssignal unterdrückt.

Bezugszeichenliste

100 Datenverarbeitungseinrichtung
10 integrierte Schaltung
12 Register
14 Programmzugriff
16 Steuereinheit
18 Leitung
20 Taktsignal
22 Steuerleitungen
24 Dateneingänge
26 Datenausgänge
28 Rechenwerk
30 erstes Operandenregister R1
32 zweites Operandenregister R2
34 Zeitachse
36 Berechnung
38 Datenein- bzw. Datenausgabe
40 Datenübergabe R1-2
42 Datenübergabe R2-1

Patentansprüche

1. Verfahren zum Betreiben einer Datenverarbeitungseinrichtung (**100**), insbesondere einer Chipkarte, mit einer integrierten Schaltung (**10**), welche in Abhängigkeit von einem Taktsignal Rechenoperationen, insbesondere kryptographische Operationen, Datenein- bzw. -ausgaben (**38**) sowie eine Datenübergabe (**40**) von bzw. zu Registern der integrierten Schaltung (**10**) ausführt, **dadurch gekennzeichnet**, dass die integrierte Schaltung (**10**) derart gesteuert wird, dass das Ausführen von Rechenoperationen einerseits und die Datenein-/-ausgabe (**38**) sowie die Datenübergabe (**40**) von Register zu Register bzw. zwischen Registern (**30, 32**) andererseits zeitlich parallel durchgeführt wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass unmittelbar vor, während und/oder unmittelbar nach der Datenübergabe von Register zu Register bzw. zwischen den Registern (**30, 32**) der integrierten Schaltung Dummyberechnungen von einem Rechenwerk (**28**) der integrierten Schaltung (**10**) ausgeführt werden, welche zufällige oder vorbestimmte Daten bearbeiten, wobei keine Daten in Register (**30, 32**) der integrierten Schaltung geschrieben werden.

3. Datenverarbeitungseinrichtung (**100**), insbesondere Chipkarte, insbesondere zum Ausführen eines Verfahrens gemäß wenigstens einem der vorhergehenden Ansprüche, mit einer integrierten Schaltung (**10**), welche in Abhängigkeit von einem Taktsignal (**20**) Rechenoperationen, insbesondere kryptographische Operationen, ausführt, wobei die integrierte Schaltung (**10**) ein Rechenwerk (**28**) mit zugeordnetem ersten Register (**30**) und Datenein- und -ausgänge (**24, 26**) aufweist, dadurch gekennzeichnet, dass ein mit dem ersten Register (**30**) verbundenes zweites Register (**32**) vorgesehen ist, welches die Datenein- und -ausgänge (**24, 26**) aufweist, wobei ferner eine Steuereinheit (**16**) mit der integrierten Schaltung (**10**) verbunden ist, welche derart ausgebildet ist, dass sie einen zeitlich parallelen Betrieb der Register (**30, 32**) zur Datenein-/-ausgabe (**38**) und Datenübergabe (**40**) von Register zu Register bzw. zwischen den Registern (**30, 32**) einerseits und Rechenoperationen (**40**) der Recheneinheit (**28**) andererseits steuert.

4. Datenverarbeitungseinrichtung (**100**) nach Anspruch 3, dadurch gekennzeichnet, dass das erste Register (**30**) ein Operandenregister des Rechenwerkes (**28**) und/oder das zweite Register (**32**) ein Operandenregister der Datenein-/-ausgabe (**38**) ist.

Hierzu 1 Seite(n) Zeichnungen

- Leerseite -

Int. Cl.[7]: G 06 F 12/14
Offenlegungstag: 6. April 2000

Fig.1

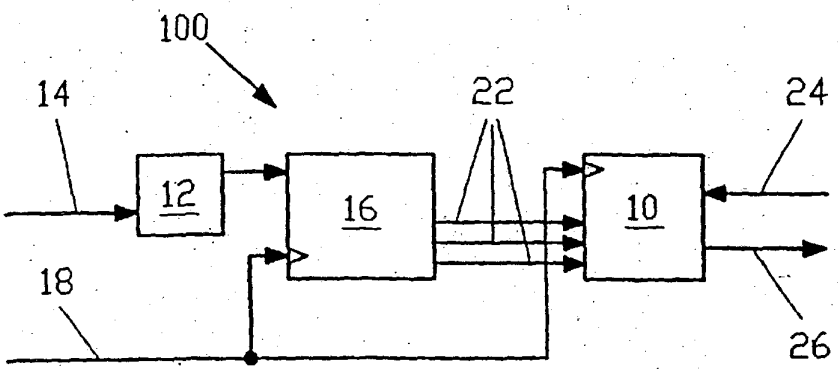


Fig.2

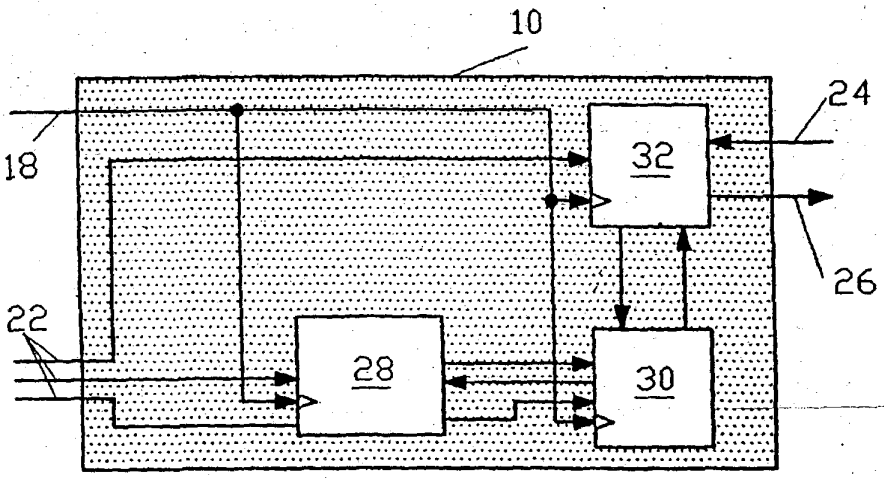


Fig.3

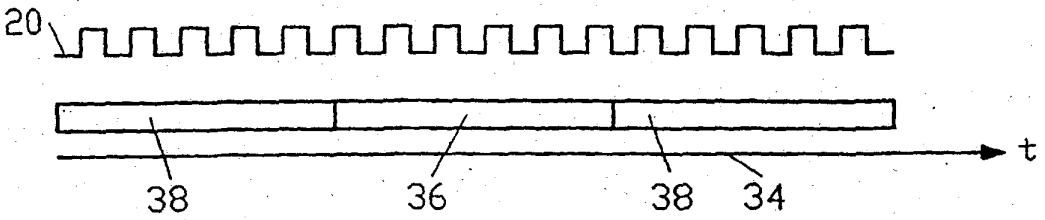
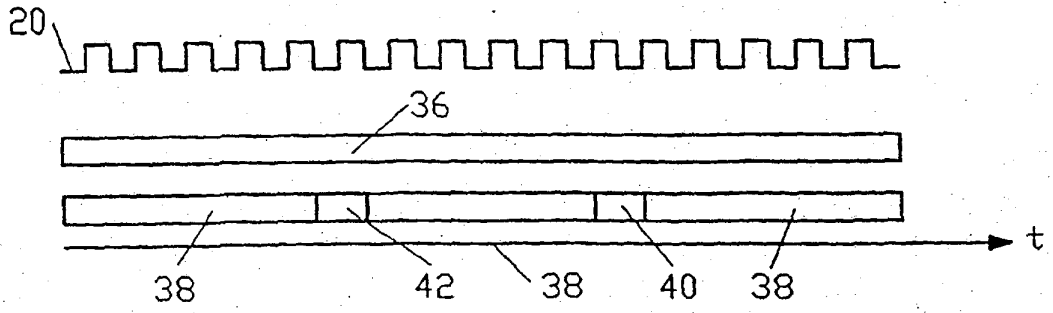


Fig.4



No English titl available.

Patent Number: DE19936939
Publication date: 2000-04-06

Inventor(s): FEUSER MARKUS (DE)
Applicant(s): PHILIPS CORP INTELLECTUAL PTY (DE)

Requested Patent: DE19936939
Application Number: DE19991036939 19990805
Priority Number(s): DE19991036939 19990805; DE19981044992 19980930
IPC Classification: G06F12/14; G06K19/073; G09C1/00
EC Classification: G06K19/073, G06F1/00N1C, G06K19/07, H04L9/06
Equivalents: EP1046142 (WO0019386), JP2002526797T, WO0019386

Abstract

The invention relates to a data processing device (100) and to a method for operating the data processing device, notably a chip card. Said device comprises an integrated circuit which in accordance with a clock pulse carries out calculating operations, especially cryptographic operations, data inputs and outputs and data transfers from and to registers of the integrated circuit. To this end the integrated circuit (10) is controlled such that the calculating operations, on the one hand, and the input/output of data and data transfer from register to register or between registers, on the other hand, are carried out time-parallel.

DOCKET NO: P2001,0023

SERIAL NO: _____

APPLICANT: Hamo Hartlieb et al.

LERNER AND GREENBERG P.A.
P.O. BOX 2480
HOLLYWOOD, FLORIDA 33022
TEL. (954) 925-1100